Cyber Today

EDITION 1, 2023

AUSTRALIA: A CYBER-HACKING TARGET

INVESTING IN CYBER RESILIENCE

THE RISE OF SPEAR PHISHING ATTACKS

AISA Australian Information Security Association

AUSCERT

SAFEGUARD YOUR INFORMATION

WITH AUSTRALIA'S PIONEER CYBER EMERGENCY RESPONSE TEAM

- Incident Management
- Phishing Take-Down
- Security Bulletins
- Security Incident Notifications
- Sensitive Information Alert
- Early Warning SMS
- Malicious URL Feed

AusCERT provides members with proactive and reactive advice and solutions to current threats and vulnerabilities. We help members prevent, detect, respond and mitigate cyber-based attacks.

As a not-for-profit security group based at The University of Queensland Australia, AusCERT delivers 24/7 service to members alongside a range of comprehensive tools to strengthen your cyber security strategy.

BECOME A MEMBER TODAY

+61 (0)7 3365 4417

MEMBERSHIP@AUSCERT.ORG.AU

AUSCERT.ORG.AU

PUBLISHED BY :

ABN 30 007 224 204

PO Box 256, North Melbourne, VIC 3051
Tel: 03 9274 4200

Email: media@executivemedia.com.au
Web: www.executivemedia.com.au

PUBLISHER
David Haratsis
david.haratsis@executivemedia.com.au

EDITOR IN CHIEF
Giulia Heppell
giulia.heppell@executivemedia.com.au

CO-EDITORS
Dr Suelette Dreyfus, Akash Mittal, Branko Ninkovic

EDITORIAL ASSISTANTS
Eden Cox, Kate Hutcheson and Ruby O'Brien

DESIGN
Sam Garland

PARTNER ORGANISATIONS
AusCERT, **Emantra**, Introspectus, **Rapid7 Australia Pty Ltd**, SANS

COVER
Adobe Stock

Contents

Foreword

A message from Mike Trovato, Director, National Board, AISA.

Mike Trovato

As I write this, we are fresh from attending the Chifley Conference of the Chifley Research Centre, a major Labor Party think tank. The conference took place on the weekend of 4–5 February at the National Press Club in Canberra, just days before the start of the 2023 federal parliamentary sittings.

In attendance was Prime Minister Anthony Albanese and Treasurer the Hon. Dr Jim Chalmers MP, along with the Minister for Finance, Minister for Women and Minister for the Public Service, Senator the. Hon Katy Gallagher; Minister for Employment and Workplace Relations, and Minister for the Arts, the Hon. Tony Burke MP; plus former Treasurer Wayne Swan and the Hon. Senator Patrick Dodson.

Chifley 2023 focused on progressive public policy thinking from the perspective of the Australian Labor Party and its international partners. The conference theme was 'Governing for Purpose: entrenching reforms, growth and inclusion'.

AISA attended Chifley as part of its advocacy and policymaking role, and there were several learnings. Chifley covered a range of sub-themes and plenary topics, including the implementation of the Uluru Voice, the key elements of inclusive growth and the lessons that progressive governments are learning while in power. It also addressed the importance of building capacity to govern and restore public sector capability.

Many key bits of information were shared, and the key themes offered focused on more and better jobs with better wages – including in the public service and entrenching important protections for workers. Chalmers spoke of his essay in *The Monthly* and the need to look closely at capitalism after the multiple crises. In a time of serial disruption – which includes major data breaches at Service NSW, Optus and Medibank – to our economy, our society and our environment, the treasurer argues for the place of values and optimism in how we rethink capitalism.

Although the key themes and messages were not about information security per se, they pointed towards a bright future for AISA members and the industry, more jobs for our industry, and ways in which we will play a greater role in building the resilience of Australia.

One of AISA's strategic focuses is to strengthen government relations in 2023. This will come from sources such as advocacy work directly to state and federal governments, industry, research, publications and events. AISA's government engagement activities must be prioritised over the next 12 months as the government's agenda is very, very ambitious.

Upcoming key initiatives are:

- Cyber Security Strategy 2020 review
- skills shortage – cadetships/intern programs
- cyber security awareness for small and medium-sized enterprises
- to assist the government with capacity building locally and internationally
- professionalisation of the cyber security industry
- key legislation/codes – all essentially stalled to some degree by change of government or delays from previous:
  - Privacy Act Reform
  - Health Identifier Review
  - Critical Infrastructure – Risk Management
  - Strengthening Cyber Security Regulation and Incentives – 2020
  - Identity Management DTA Digital Identity – 2021
  - Reform of Electronic Surveillance Framework.

Again, it is an ambitious agenda. We urge all members interested to take part and support our efforts.

Please enjoy this new issue of *Cyber Today* and continue the great work of building a more resilient Australia. •

AUSTRALIAN CYBER CONFERENCE 2023

MELBOURNE | 17 – 19 OCTOBER

Melbourne Convention and Exhibition Centre

DON'T MISS THE **CYBER EVENT OF THE YEAR!**

INTERNATIONAL KEYNOTE SPEAKERS
4,000+ DELEGATES • 400+ SPEAKERS

SUPER SAVER REGISTRATIONS
and Call for Papers
open 22 March 2023

#cybercon2023
cyberconference.com.au

OPPORTUNITIES

AISA

What am I walking into?

BY ROB DOOLEY, VICE PRESIDENT ASIA-PACIFIC AND JAPAN, RAPID7

How to prepare for your first CISO role.

I've become close friends with a lot of CISOs over my years in cyber security, and they often call when they move into a new role. It's an intense time, and they find it useful to discuss what they should prioritise and how they can balance listening and learning with acting and delivering change. Here are some tips from those calls for any incoming CISOs out there.

Prepare before you start

The job starts when you accept the offer. Begin learning about the company and your starting point. Is the focus of the job technical or transformative? What's the cyber security culture? What's the business strategy? And how does that affect cyber security posture? Understanding the organisation's cyber maturity offers you a distinct advantage come day one.

Assessment and triage

Once you start, it's time for a more thorough assessment. Learn from your new colleagues in IT, digital or risk. Listen to their experience and discuss needs with the other business leaders.

Next is the initial triage of the environment. You need a true picture of assets, data and controls to inform your plans. That requires interrogating data from your security information and event management platform, or working with partners to collect and analyse security telemetry.

Now, you can begin working with your teams and C-suite peers to put plans in place.

Set your goals

Your initial goals depend on the context. If you are the organisation's first security leader, you may develop the company's information security policy. But if you are coming in after a major incident, you may have to lead the review and remediation process.

Quick wins show impact and get buy-in from stakeholders for future improvements. Working with software-as-a-service providers with broad capabilities will be critical in those first few months. They'll be able to deploy solutions at speed to improve security maturity and decrease risk. You'll also benefit from economies of scale, expertise and knowledge that they have from dealing with similar organisations.

With the basics and day-to-day security in hand, think further ahead. Set your vision for the organisation with a road map for the next two years, and operationalise security for more value and efficiency.

Communicate up, down and across

New CISOs often make the jump from within a security operations centre or leading risk teams. As you venture into the new role, it's your team that implements your strategy, so take the time to get to know them, and communicate your expectations and objectives clearly.

How you engage with senior leadership will influence your success – whether that's securing budget for resources or changing culture. Boards and company executives prefer to consume proposals in the context of the company's strategy, so you must be fluent in business strategy, as well as technology.

Growing in stature

Becoming a CISO is a big step. But it's a fascinating and rewarding job, and, as the function matures further, its stature will only increase and prove to be of immense benefit to businesses everywhere. ●

The wisdom of the crowds coming through loud and clear at CyberCon2022

BY JENNIE VICKERS

Back in 2004, James Surowiecki published the book *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations.*

Ideas around the benefits of collective wisdom ring true at conferences and tradeshows where line-ups of technical experts converge to share their thoughts and ideas. With over 30 topic streams and hundreds of speakers, there was more than enough on CyberCon's agenda to provoke new ideas and build a plan of action for 2023.

But one can't be everywhere, so I've carefully identified a number of themes inspired by several of the speaker presentations, which will be of interest to security professionals when they wind back up after a well-deserved summer break.

'Cyberworthiness': Adopting a philosophy from aviators

In his presentation, Squadron Leader Arjun Xavier of the Royal Australian Air Force introduced the idea of 'cyberworthiness'. The 'worthiness' concept is familiar to many in the context of air and sea, but this extension into cyber provides a useful framework.

It is, in essence, a risk management and continuous improvement framework, enabling the Australian Defence Force to effectively manage risk in cyberspace as it executes its mission. An underpin is 'Don't get chained to compliance.'

Arjun explained that cyberworthiness is not just about security. Traditional cyber security is focused on activities designed to ensure the confidentiality, integrity and availability of systems. Cyberworthiness, on the other hand, 'is rooted in survivability –

CyberCon2022, Melbourne

business continuity, in corporate terms – and assurance of our mission'.

For all of us, our future cyberworthiness governance framework needs to be scoped across three key pillars – people, processes and technology (the reflections of 'Sully' Sullenberger – refer to my other article on page 12 – around airworthiness changes from 45 years ago would indicate that many organisations have a long way to go in understanding the people side of this puzzle).

Group efforts, partnerships and collaborations

A confession: I am hooked on a Netflix Korean drama called *Vincenzo*. It is about a Korean-born mafia consigliore in Seoul. The point of this reference is that the series demonstrates the many ways in which the mafia and other crime groups (pre-cyber) around the world have always collaborated and worked in partnership, where it is of value to them to do so.

A number of speakers at CyberCon2022 alluded to the importance of the good guys (us) getting as good at collaboration as the hackers. Many of them recognised that we're still not as good as we need to be.

The idea of being out played in this regard was reinforced when speaker Glenn Maiden explained the work of Fortinet as part of the World Economic Forum's (WEF) Cyber Atlas Project.

'Defeating global cybercriminal organisations requires a global group effort with strong, trusted relationships among cyber security stakeholders,' says the WEF. 'Criminal enterprises function almost exactly like corporations. Once attackers start to quit out of fear of being exposed and arrested, or

feel the profits aren't worth the risks, then cybercrime may begin to recede.'

Several different speakers from Accenture shared this view of the need for better collaboration, recognising that 'visibility across enterprises and government agencies is also essential to allow common goals, training and governance to be implemented, and to reduce duplicated efforts'. The reality is that cybercrime as a service (CaaS) is growing faster than software as a service (SaaS)!

Continuing cyber ignorance

Paula Januszkiewicz is a rockstar MS Security Enterprise Expert, who both delivered a keynote and ran half-day workshops. Interviewing Januszkiewicz, we got around to a key dilemma facing executives embracing digital transformations and Internet of Things (IoT) where the risks are rising.

Januszkiewicz's view is that if we apply strict security rules, no-one will be able to get any work done, so a balance needs to be struck between safety, usability and practicality. If executives do not understand the underlying technology, striking that right balance is hard.

Cyber focus at a government level

In her opening speech, the Hon. Clare O'Neil MP, Australia's Minister for Home Affairs and Minister for Cyber Security, said that the 'new government in Australia has made the decision to have a cyber security minister because we want to elevate this issue to the level of importance that it so clearly is for Australia's business, for Australia's citizens, and very much for our nation'.

'Cyber is everything and it is everywhere,' she told the CyberCon2022 audience. 'A resilient cyber ecosystem is going to be fundamental to our country's future.'

We need a champion of cyber from government in New Zealand.

CyberCon2022, Melbourne

2023: Try telling a different cyber story

Mina Zaki from KPMG ran a useful session on how to use storytelling to change the narrative. She made the case for well-reasoned, relevant and problem-focused case studies along with a better understanding of the way a story engages brains.

Elevate security issues to board-level concerns and language

Talking about changing the narrative, Michael Shepherd from Accenture commented that: 'Essentially, it boils down to catalysing the business relevance, capturing the strategic picture of cyber security with the right scorecard, and speaking the language of business impact in all cyber security communications to the board.'

Jason Brown, Principal Advisor, Security and Risk to the Board of Thales ANZ, reminded us that, 'It's not about compliance, it's about survival in a dangerous and complex world.'

Persia Navidi of Hicksons lawyers noted – with thoughts heavily laden with animal references – that 'when it comes to board directors, it goes without saying that cyber events are no longer "black swan" events, but despite this, they're still very much treated as the elephant in the room'.

Securing critical infrastructure

Amy Ormrod and Zoe Thompson from PwC were joined by colleagues from Europe for a global perspective. A few key takeaway thoughts included:

- If you can't map your asset interdependencies, you have no way of understanding what is critical.
- You need a security-by-design lens across the entire organisation.

- Internal silos are more of a threat than the external threats.
- Manage expectations – spend is never going down.
- Where is CI data? Is there a war coming near your data?

Is it time for your board's committees to play a greater role?

Ashwin Pal of RSM Australia is a friend of New Zealand, having previously spoken at the New Zealand Defence Force/New Zealand Defence Industry Association's IDEAS 2020 event. He presented on the role of Audit and Risk Committees of Boards (ARCs). Pal's summary points are a useful list:

- Cyber security is a key business risk and must be treated as such.
- As a result, board/ARC members' responsibility for cyber security is increasing.
- Board/ARC members MUST ask the right questions of management and THEMSELVES to be able to discharge their duties.
- Cyber risk needs to be quantified so it can be managed.
- A methodical program is necessary to stay on top.
- You cannot control what you cannot measure.

'Boards and executives must treat cyber risk as a high-priority business risk,' he said in closing. 'It must be part of the Enterprise Risk Management framework, with risk appetite clearly defined and cyber risk mitigated to an acceptable level. Unless this methodical approach is taken, breaches will continue to increase.'

Data: How about we go with effective de-identification for now?

Dr Ian Oppermann, the New South Wales Chief Data Scientist, delved into the vexing issue of personal information and the failures of de-identification attempts. Enter stage left, the PIF Project Tool. This project is a collaboration between the Cyber Security CRC, CSIRO's Data61, the Australian Computer Society, and the New South Wales and Western Australia governments.

'The Personal Information Factor (PIF) Tool measures the risk associated with releasing a dataset,' explained Dr Oppermann. 'When risks are high, an artifical intelligence–enabled tool analyses attack vectors and transforms the data, using provable privacy perturbation techniques, making it suitable for publication.'

CyberCon2022, Melbourne

Procurement: How to pick the right security horse

Mark Hofman, CTO of CyberCX, caused a few OMG moments. I never say OMG, but in this case, Hofman shared the results of a Gartner report from July 2022, which found that 56 per cent of organisations said they had a high degree of purchase regret over their largest tech-related purchase in the last two years. This is shocking but credible.

Hofman had screeds of good advice but to vendors he said, 'get better at articulating both your licensing model and the problems you actually solve; and to buyers the usual entreaty to get better at articulating requirements but also ensure a whole cross organisation team is involved in the procurement.'

Final thoughts: We need more sessions on convergence

It really is time for events in 2023 to get better at combining OT and IT, and talk convergence across the whole spectrum. The events organised by associations are better placed to make this happen... and it needs to, as a matter of urgency. •

This article was originally published in New Zealand Security Magazine.

Trends in cyberthreats

Think of the major world changes this century – globalisation, geopolitical instability, terrorism, social media and the digitisation of lifestyle. Each of these dynamics has harboured the growth of a cybercrime industry now estimated to be worth US$8 trillion.[1]

Even climate change and COVID-19, which led to changes in the way we live and work, have created new vulnerabilities for cybercriminals to exploit.

The growing sophistication of cyber attacks and involvement of state-sponsored actors make it harder for organisations to defend. Here are some increasing or emerging trends to be aware of:

- Cyberwarfare and espionage techniques, now funded by national defence budgets, will increasingly turn eyes from the military to the marketplace not only to disrupt, but also to gain self-funding through direct exploitation. This will create a vicious circle.
- The emergence of a viable Cybercrime-as-a-Service business model significantly lowers the barrier of entry for unsophisticated mass hackers. Many threats, such as distributed denial of service, phishing and malware, are now productised on the dark web, together with support and technical assistance.
- Internet of Things devices, which are ubiquitous, are subject to increasing attention, often because they are seen as the 'easy way in' to a company network. From electric vehicle chargers, point of sale, and physical security and measurement devices, to cameras and implanted medical devices, there exists serious potential for extortion, including life and death threats.
- Supply chain cybercrime has potential for disruption on an industrial scale. Even small players in a critical supply chain (often the weakest link) are targeted – not because of the direct reward, but because of the collateral damage that can result elsewhere.
- The massive artificial intelligence (AI) of global clouds is being exploited to host resource-heavy capabilities, such as brute-force computers, machine learning, botnet-as-a-service, Domain Name System laundering, etc., which can create deeper and smarter types of exploits. Another product of AI – deepfake – makes phishing, scamming and identity theft harder to defend against.
- That old chestnut, ransomware has proven so easy and lucrative. Emerging is the concept of double extortion, where the data is not only held to ransom, but is also offered for sale on the dark web at the same time. Two birds with one stone. Ransomware is now being developed to target specific sectors, such as healthcare, education and government.
- As opposed to steal and run, the advanced persistent threat technique doesn't require immediate pay-off. For example, an agent is allowed to sit dormant on a victim's network, waiting for a trigger. In the meantime, they can perform legitimate tasks to disguise their real intent. Criminal groups using this model are sophisticated and must be well funded, as the 'time to payout' is long. Known perpetrators of this activity include APT28/29, APT10, APT33/34 and Lazarus Group. All of these are state-sponsored.

You won't be subject to all these threats, but some may be likely. The best defence is to know what's out there, which risks your business or market is most susceptible to, and to stay close to expert advice.

Emantra has experience in dealing with many of the emerging threats mentioned here, and can give you a risk-weighted scorecard and specialist advice. ●

1 2022 Official Cybercrime Report, Cybersecurity Ventures

Emantra
SECURING OUR FUTURE

We are EMANTRA

Sovereign Hosting
Secure Cloud
IRAP-Assessed SIG
Enterprise Cyber Risk Management

1300 728 953

What next after resilience?

BY JENNIE VICKERS

Wisdom from AISA CyberCon2022.

Remember when you were 11 and you went back to school after the holidays, and saw friends and shared experiences? You may recall the din and the excitement. That was how it was at CyberCon2022 in Melbourne, after two long years away.

I vaguely recall that the school return thrill lasted less than a day, but I can report that the electricity of reconnecting continued for the full three days.

The theme of the event was 'Resilience in the Cyber World'. A good theme and a topic we continue to grapple with.

An event attracting thousands is able to bring in big global speakers, and AISA did not disappoint. To wrap up 2022 and maybe to help frame our resolutions for 2023, here is a selection of thoughts, ideas and sound bites from a selection of these globally recognised speakers.

Captain Chesley 'Sully' Sullenberger

Ric Elias of North Carolina was a passenger in row one on Flight 1549, which crash-landed 13 years ago on the Hudson River in New York City. This experience of having no control over his next 3.5 minutes, and having his life in someone else's hands, changed his life.

He was not a speaker at CyberCon2022; however, the pilot that day was Captain Chesley 'Sully' Sullenberger, who was the closing speaker of the event.

Within minutes of commencing his address, Sully stressed that this Hudson River miracle required the efforts of a whole team, including the first officer, Jeffrey Skiles, the crew, the passengers, and everyone on the ground. That success was as much a result of teamwork and adherence to procedure as it was of skill and coolness under pressure.

Sully pointed out that they had just 3.5 minutes to find a solution that was not in

Image courtesy AISA/Magnetic Shots

the checklists or manuals, but behind those 3.5 minutes was a lifetime of learning.

He explained that approximately 45 years ago, aviation safety changed with the introduction of a raft of new ideas around the role of people. The focus came onto the idea of 'turning a team of experts into an expert team'. They recognised that compliance alone is a necessary but not sufficient condition for safety.

'We also had to have the resilience, and other systems and knowledge to be able to handle things we hadn't trained for or envisaged,' Sully told his audience.

Another set of changes involved reducing the flight hierarchy between the captain and the rest of the crew. They made it psychologically safe for the most junior member of a team to approach a captain about an issue. They made it 'about what is right, not who is right'. There was a dual right to speak but also the responsibility to speak up.

Jumping back to recall his Air Force days and being a fighter pilot working in fast-speed, low-altitude formations, he pointed out that the real learning from rapidly unfolding events and experiences occurred at the post-flight debriefs, where leaders and followers held each other to account.

Those brutally honest exchanges about what worked or didn't and why made the difference. The lessons learnt process is why aviation has been so safe for many years, and this is an essential part of an airworthiness system.

During the Q&A session, the obvious parallels to cyber events were drawn, and it was clear that too few in the audience saw this approach paralleled in their organisation, but many clearly thought it should.

Erin Brockovich

Earlier in the event, the keynote speaker was Erin Brockovich, known to many thanks to the movie starring Julia Roberts, and now to many millions more as an environmental activist and passionate advocate for protecting water as a fundamental human right.

Brockovich was quick to identify that she was not in the room to talk about cyber security, but was there to share her thinking, which was relevant to security. Her big opening volley was around the

need to go back to listening to our instincts, using intuition, and being connected to our environment, people and ourselves. With a rare suggestion, she identified an unexpected benefit of COVID-19 to the world in that it sat us down, triggered a reboot and reset, and forced us to be more awake to our environment.

Published during COVID-19, her book, *Superman's Not Coming*, is about US water and infrastructure issues, but has relevance to everyone concerned about security issues in their organisation or life. 'Whatever we do, we keep looking for someone else to give us the answers when the answer lies within the person in the mirror,' she said.

Brockovich introduced a term unknown to most of us in the room: 'sticktoitiveness'. Yes, it is a real word, and it means dogged persistence and perseverance. 'This humanistic sense is all about using intuition, to follow what does not feel right.'

On leadership, Brockovich's philosophy is that it is not about being up the front, but rather about seeing the quality in another and pulling them in to work with you. 'I want to come in and work with you, how do we collectively get something done?' If you are worried about cyber, 'you ask questions, you plan, you be prepared, you implement an action'.

Brockovich admitted that she was freaking out a little about speaking to a cyber community, so she went to her bank and asked them whether it was a 'big thing'. The manager said cyber is all they do, and shared a story of a fraud. The skills that caught it before it was too late were all those she talks about.

'Be you, be present. If something does not feel right, if you are uncertain, step out of that box,' she said. 'Never be afraid to activate your own instincts, rely on them, work with them, believe them.'

Answering a question about how to get people to listen to hard truths about security risks, her advice was to allow space for people to process and give them facts, but recognise that people struggle to believe truths if they are driven by fear.

Steve Wozniak

Steve Wozniak (Woz) is a rare speaker who can provoke a large auditorium full of people to smile and keep smiling. He was his authentic self and did not talk in sound bites. Sharing stories of Apple's history, he reminded us that the iPhone was the greatest product introduction ever. 'I've got more power than Superman with my iPhone...' (We possibly need to connect him with Erin Brockovich!)

My favourite thing he said had resonance for everyone going into the holidays and thinking about the person they wanted to be in 2023. His consistent message for the past decades (see his interview in *The Guardian* from 2016) is: 'Everything you do should have an element of fun in it. Happiness to me is smiles minus frowns (H=S-F). Increase your smiles, do a lot of fun things, enjoy entertainment, talk with people, make jokes. That's creativity.' No more frowning in 2023!

Ric Elias

Finally, to Ric Elias. Apart from co-founding Red Ventures, a portfolio of digital companies in North Carolina in 2000 that has grown to 3000 employees across several countries, Elias is a survivor of aforementioned Flight 1549.

These days, as a result of his near-miss experience, he runs a portfolio of tech brands with a strong social focus. His four-minute TedTalk from TED2011 is worth a quick listen. It is entitled '3 things I learned while my plane crashed'. Sully's wisdom comes from the cockpit, from a position of leadership and a place of control. Elias's wisdom comes from the back end of the plane, where there's a complete absence of control.

Wisdom from Elias includes:

- Live with purpose, on purpose.
- This moment is the only one that's guaranteed.
- If we live each day like we are running out of time, making every second count, we will live with no regrets.
- Compete only against who you were yesterday. There will always be someone who is smarter, stronger, or luckier – but what matters most isn't winning.
- Give your best to the work that's worth doing, so you can earn the right to keep doing it.

Leader or follower, this combined wisdom has something for everyone. •

This article was originally published in New Zealand Security Magazine.

Benefits of a systems-thinking approach to threat modelling

BY MICHAEL COLLINS

Michael Collins

Most, if not all, cyber security experts can relate to the age-old adage that 'the only constant in today's world is change'. Threat actors are always innovating and improving their techniques to find new ways to breach systems, while defenders must adapt and seek better ways to secure a system. Businesses driven by digital transformation are increasingly interconnected across numerous public clouds, and the relative simplicity with which business teams can acquire software as a service ensures that organisational boundaries are constantly shifting.

What is threat modelling?

To successfully safeguard an organisation's systems, a defender must have visibility into the system's assets and associated vulnerabilities, and potential threats to them. Threat modelling is a method of documenting the threat landscape that many cyber security professionals overlook. Threat modelling is a security-focused perspective of the application and its environment – essentially a visual representation of the system you are attempting to safeguard that helps you to investigate where attackers may exploit structural weaknesses.[1]

Visualising the system through mapping is important because it helps you get a better understanding of the system you're thinking about. It's like creating a 'mental model' of the system, and research has shown that it's a better way to communicate it to others than just writing or speaking about it.[2]

What is systems thinking?

Systems thinking is the art and science of seeing the world as a complex interconnected system, exploring how these systems work, and uncovering new opportunities and solutions. One of the core concepts in the study of complex systems is emergence. Emergence refers to how the system's behaviour emerges from the combined interactions between its parts (actors or agents). Systems thinking is not just about observing and describing a system, it is about understanding the system and how it functions before attempting to solve problems or create a solution.

Complex adaptive systems are one of nature's most effective solutions, so there are plenty of examples of this in biology. Ant colonies can handle very complex tasks with no centralised authority, no systematic plan, or any kind of government. Each ant plays a role in decision-making: should it forage, take out the trash or defend the nest? Every ant is connected with the others, and the interactions are mostly local, following simple rules. What emerges from this collective behaviour is an ant colony, which, when observed at the colony level, has the hallmark characteristics of an organism. It's resilient, adaptable, and has its own life cycle. Still, the single ant is only dealing with local data and interaction, and has no awareness of the global system. This is what makes complex adaptive systems so difficult to comprehend – emergence hides the cause and effect.

Similarly, failing to appreciate the complexity of the technology system you are threat modelling may have unexpected consequences, such as poorly designed controls, flaws in your defences, or a failure to consider the various threat actors that may target your system.

In other words, systems thinking is about building mental models that better align with real-world systems, through a process of structuring the information we have, testing that through feedback and iteratively updating it so that our mental model is a better approximation of reality. The information we get as feedback from the real world is critically important; but what we do with this information – how we structure it – is what makes a mental model.

DSRP: The four rules of systems thinking

More than two decades of research conducted by Dr Derek Cabrera of Cornell University[3] went into discovering that of the thousands of different systems frameworks, methodologies, theories and practices, there are four simple rules that underlie systems thinking. These go by the acronym 'DSRP'.

Most importantly, the four rules of DSRP are required for you to even form an idea, and if you were unable to use just one of these it would be nearly impossible to think, let alone do the simplest of tasks.

- **Distinctions rule:** Any idea or thing can be distinguished from the other ideas or

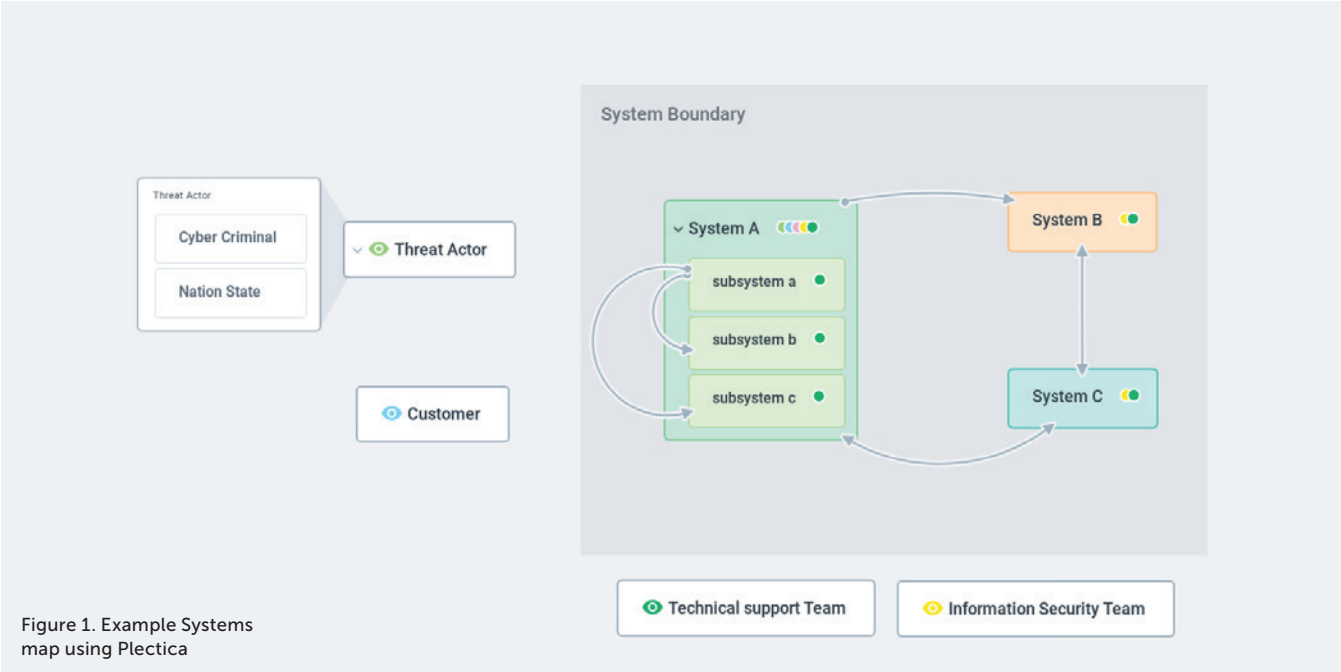


Figure 1. Example Systems map using Plectica

things it is with. When you distinguish one thing from another thing, you create a boundary. In threat modelling, this could relate to the boundaries you draw around the system, identifying which parts of the system are within the boundary and, therefore, what is outside the boundary.

- **Systems rule:** Any idea or thing can be split into parts or lumped into a whole. What are the parts of the whole system, what are the parts of those parts, or what is the system a part of? This is like zooming in on the system map to see more detail, or zooming out to understand it's context in the larger scheme of things.
- **Relationships rule:** Any idea or thing can relate to other things or ideas. It is difficult to understand how any system works if you do not understand the relationships between the parts of the system. All relationships require us to understand the action/reaction or cause/effect relationships between them, and whether they are causal, feedback, inputs or outputs, direct or indirect.
- **Perspectives rule:** Any thing or idea can be the point or the view of a perspective. Perspectives help us expand our thinking to include more options (divergent thinking) and to narrow or create greater focus (convergent thinking). Threat modelling often draws the boundary from a security perspective, but would an attacker draw the same boundary? Being able to decipher what your enemy sees and doesn't, what they are aware of and not, what they value and don't, and how they see you and not, is part and parcel of advantage.

How to apply systems thinking to threat modelling

To apply systems thinking to threat modelling, begin by visually mapping the system you're trying to model. For example, if you're threat modelling an application, you need to map the application's architecture and the set of potential users.

You can do this on a whiteboard, Post-it Notes or the back of a napkin, or using software like Plectica (Figure 1).

Apply the four rules of systems thinking to understand the system better. Research shows that asking the following five DSRP questions of an idea, issue or concept increases systems thinking.

1. What things am I choosing to see and not see?
2. How are these things organised into part-whole groups?
3. How are these things related? (And not related?)
4. Do these relationships have parts?
5. From what or whose perspective?

DSRP questioning helps us to see things about systems, and also to consider some of the things we are not seeing. It also helps us to look at systems from multiple

perspectives. When we do look at things from multiple perspectives, it doesn't just shift the point of view – it also changes the distinctions we make, the relationships we do or do not see, and the way we organise parts into a coherent whole.

How systems thinking can improve threat modelling

Systems thinking can improve threat modelling in two ways: by deepening your understanding of the system, and by expanding your creativity while exploring the system.

Understanding the system better

When you apply the four rules of systems thinking to the system you're trying to threat model, you better understand the system's interconnectedness and interrelationships. You identify feedback loops and other connections that might be overlooked in a traditional threat modelling approach.

Expanding creativity while exploring the system

The rules of systems thinking can also expand your creativity as you look for vulnerabilities in the system. This divergent thinking can help you uncover threats that you might have overlooked in a traditional threat modelling approach.

Deepen learning

When you apply the rules of systems thinking, you deepen your understanding of the system, which will help you retain more knowledge of the system. This will help you adapt to changing threats more quickly and efficiently.

Conclusion

With the increased frequency of cyber attacks, the stakes are getting higher for organisations every day, so it is even more important that your understanding of the system reflects reality.

Systems thinking is an incredible method to improve threat modelling; and by applying the four DSRP rules to your models, you will not only produce better threat models, but you will also become a more systematic thinker in other aspects of your life.

In cyber security, thinking isn't optional, so how you think matters. •

About the author

Michael Collins *is a seasoned cyber security expert with over two decades of industry experience. Collins's experience covers multiple countries, from the United Kingdom to New Zealand, and includes work in both small and medium-sized enterprises, and Fortune 50 global corporations. Collins has significant expertise in scaling cyber security capabilities within financial services customers, and presently serves as CISO for Judo Bank. Collins is frequently engaged for expert advisory services, and serves as a security adviser to boards and startups. Collins holds a Postgraduate Certificate in Strategic Planning, GIAC Certified Security Leadership and Applied Information Economics, and is certified in red team thinking and systems thinking. Collins gives back to the industry by mentoring the next generation of cyber security experts, and regularly shares his thoughts via the Cyber Cognition™ blog.*

References

1 https://owasp.org/www-community/Threat_Modeling

2 Mayer, Richard E., *The Cambridge Handbook of Multimedia Learning: Cognitive Theory of Multimedia Learning*, 2005

3 Cabrera, D. & Cabrera, L. (2018) *Systems Thinking Made Simple: New Hope for Solving Wicked Problems in a Complex World* [2nd edition]. Odyssean Press. Ithaca, NY.

Australia: a cyber-hacking target

BY ROSEMARY SINCLAIR AM, CEO, .AU DOMAIN ADMINISTRATION (auDA)

Is Australian consumer and small business cyber readiness up to scratch?

Whether you're young or old, live in a regional town or metropolitan city, run your own business, are a tradesperson or work in an office, research shows that you use and rely on the internet for your everyday life. Unfortunately for many, concerns about cyber security are getting in the way of fully realising the benefits of the internet.

.au: critical Australian infrastructure

The .au Domain Name System (DNS) is critical Australian infrastructure that underpins the internet as we know it today. It provides a gateway to online services that are vital to modern society, such as web browsing, email, ecommerce, web-based applications, and business functions, including order management and automation.

Rosemary Sinclair AM

The .au DNS, powered by auDA, ensures that people worldwide have seamless access to the internet services they need, when they need them. With more than four million registered .au domain names and .au DNS servers responding to an average of 2.6 billion DNS queries each day, security is a key priority.

It is important that we keep the .au secure to keep you – and many other billions of internet users – online.

We know that online security is important to Australians, and this was evident in the results of auDA's recent Digital Lives of Australians[1] research study.

Central role of the internet for Australians

The Digital Lives of Australians study is an in-depth exploration of the online experiences of Australian consumers and small businesses.

The 2022 report confirmed what many of us know – that the vast majority of Australians use and value the internet. Findings include:

- 98 per cent of consumers say the internet adds value to their lives
- 61 per cent of working Australians could not do their job without the internet
- 84 per cent of small businesses would struggle to survive without the internet.

We only need to read the daily news to understand that cyber security has never been more topical, nor have robust cyber security measures ever been more urgent and important

Unfortunately, the rapid development of technologies and their integration into our lives has meant that the challenge of keeping users secure online has also increased.

Cyberthreats on the rise

We only need to read the daily news to understand that cyber security has never been more topical, nor have robust cyber security measures ever been more urgent and important.

The Australian Cyber Security Centre's 2021–22 Annual Cyber Threat Report shows that a cyber attack is reported every seven minutes. This is up from every eight minutes the year prior, and every 10 minutes the year before that. Without action, this rate will continue to climb.

Addressing cyber security threats will require leadership from the top levels of government and the technology industry, but there is a role for each of us – across all levels of industry – to work together to empower individuals and small businesses with the knowledge and tools to protect themselves.

Cyber security is an ever-present concern

The Digital Lives of Australians 2022 report shows that cyber security is an ever-present concern that undermines consumer confidence in using the internet. Of consumers surveyed:

- four out of five are concerned about their personal data being stolen, and three-quarters have concerns about online privacy
- three-quarters agreed that cybercriminals are becoming smarter and more sophisticated
- only half feel confident that they have safeguards in place to keep their personal data secure online.

Of small businesses surveyed:

- almost one-third consider online scams and the security of their business data to be major concerns
- less than half feel very confident with processes to protect their online security
- fewer than one-quarter have a cyber security policy in place or provide staff with cyber security training
- almost one-fifth spend nothing at all on cyber security.

This should be of concern to businesses as they increasingly move services, as well as staff and customer engagement, online. As one research participant and Sydney-based sole trader noted, having twice been the victim of cybercrime, they no longer accept online payments and now only accept in-person cash payments or bank transfers.

Another small business owner from regional Victoria noted that the exposure of staff or customer details would be a 'serious problem that would shake their confidence in our ability to be a trusted business'. An older Australian from regional New South Wales shared this same

fear of information being stolen, telling us: 'I worry about having my information used to create false identities.'

Build confidence, boost security

Despite their concerns, the majority of consumers and small businesses are not aware of trusted, readily available cyber security tools and resources. For example, only six per cent of consumers and 12 per cent of small businesses had used government resources to educate themselves on online security in the three months prior to our survey.

Interestingly, the survey found that the small percentage of consumer and small business respondents who did access trusted government resources were significantly more confident in using the internet overall.

The research also showed that those who are more confident in managing their cyber security are more confident using the internet overall.

While we are unable to draw a causal relationship from the research, this correlation indicates that there is a significant opportunity to improve confidence among Australia's internet users by building cyber security knowledge.

A role for industry

auDA's Digital Lives of Australians research provides a thorough understanding of the benefits and challenges of the internet for Australians. Through the research, we aim to generate discussion and action within industry, business, government and education sectors to improve how Australians access and benefit from the internet.

Equipped with this deeper understanding, industry can continue to drive solutions to cyber security concerns. Industry players both big and small can contribute by building innovative new tools, investing in skills development, and promoting the take-up of practical, effective cyber security practices among Australian consumers and small businesses.

Together as an industry, we look forward to supporting Australians to achieve a more secure online future. •

References
1 https://www.auda.org.au/DL22

AusCERT – a proud history and a bright future

AusCERT is a world-renowned organisation that has been providing cyber security services and expertise to small and large businesses, universities, and government agencies in Australia and neighbouring countries for almost three decades. Since its establishment in 1993, AusCERT has built a reputation as a trusted adviser and a provider of critical incident response and security analysis services. In March this year, AusCERT shed its 'young adulthood' status and celebrated its 30th birthday!

AusCERT's history is rooted in its mission to protect the digital assets of its members by providing practical and expert cyber security advice and support. Over the years, AusCERT has responded to thousands of cyber incidents, and has worked tirelessly to develop and promote cyber security awareness, education, and best practices – both locally and internationally.

Most importantly, AusCERT is a not-for-profit organisation that exists only for its members, providing unique cyber security services that complement government and commercially available offerings. Based at The University of Queensland (UQ), AusCERT works closely with UQ Cyber and global networks, such as APCERT and FIRST, having built excellent relationships worldwide over nearly 30 years. AusCERT funds the provision of its cyber security services from not-for-profit membership fees, reinvesting a small surplus into the development of its team members, with emphasis on continuous learning and improvement in culture.

Generous sponsors allow AusCERT to host the longest-running cyber security conference in Australia each year since 2002. Known for its great atmosphere and opportunities to collaborate with peers in all industries, presentations and tutorials are sourced from the very best practitioners locally and worldwide. Members receive free or discounted attendance to excellent, low-cost professional learning and development in a welcoming environment. Registrations for the 2023 event open soon!

In recent years, AusCERT has expanded its services to include a range of cyber security training courses. With the growing demand for cyber security expertise, the AusCERT Education program has become increasingly important, providing individuals and organisations with the skills and knowledge they need to stay ahead of the rapidly evolving cyberthreat landscape.

The AusCERT Education program ranges from an introductory course for IT professionals who wish to learn the current terminology, practices and controls in cyber security; to more advanced training, such as cyber security risk management and forming an incident response plan. In recognition of the critical importance of areas such as board and executive cyber security awareness, and data governance practices, AusCERT will expand its education programs into these areas in 2023.

Together with this new direction in the AusCERT Education program, other future services will include briefings for board members and executives, and implementation assistance for data governance practices. Overall, AusCERT's direction is to continue providing not-for-profit, high-quality cyber security services and education for its members. •

AUSCERT

SAFEGUARD YOUR INFORMATION

WITH AUSTRALIA'S PIONEER CYBER EMERGENCY RESPONSE TEAM

- Incident Management
- Phishing Take-Down
- Security Bulletins
- Security Incident Notifications
- Sensitive Information Alert
- Early Warning SMS
- Malicious URL Feed

AusCERT provides members with proactive and reactive advice and solutions to current threats and vulnerabilities. We help members prevent, detect, respond and mitigate cyber-based attacks.

As a not-for-profit security group based at The University of Queensland Australia, AusCERT delivers 24/7 service to members alongside a range of comprehensive tools to strengthen your cyber security strategy.

BECOME A MEMBER TODAY

07 3365 4417

MEMBERSHIP@AUSCERT.ORG.AU

AUSCERT.ORG.AU

AUSCERT EDUCATION

Enhance your knowledge with our exceptional online training offerings for individuals and organisations (delivered in two half-day sessions).

INTRO TO CYBER FOR IT PROFESSIONALS

Understand information security principles, cyber security as a risk to business objectives; and cultivate an appreciation of the current cyber threat landscape.

CYBER SECURITY RISK MANAGEMENT

Gain the confidence to perform a risk assessment of cyber security risks and the ability to rate and assess business risks rather than technical vulnerabilities.

INCIDENT RESPONSE PLANNING

Be equipped with the tools to write and implement a bespoke incident response plan for your organisation.

BOOK ONLINE

AUSCERT.ORG.AU/SERVICES/AUSCERT-EDUCATION

Investing in cyber resilience

BY SIMON MITCHELL AND LAURA BACON

How directors are building cyber resilience and meeting the expectations of regulators and the community.

Simon Mitchell

Laura Bacon

The Australian Institute of Company Directors' (AICD's) membership of 50,000 reflects the diversity of Australia's director community, comprising directors and leaders of not-for-profits (NFPs); large, and small and medium-sized enterprises (SMEs); and the government sector. Over the past three years, the AICD has engaged extensively with this membership base on cyber security governance and regulation, through both member research, and the development of practical guidance and tools to assist Australian directors.

This engagement has revealed that Australian directors are highly motivated to enhance the cyber resilience of the organisations they govern, and separately improve their individual knowledge of cyber security governance practices. The AICD's biannual Director Sentiment Index has consistently found that cybercrime and data theft are the top issues keeping directors 'awake at night'. Separately, joint AICD–AISA research, published in June 2022, revealed that three-quarters of directors listed cyber security as a high priority for their boards, and this has resulted in increased investment in cyber resilience.

Cyber Security Governance Principles

In October 2022, the AICD, in collaboration with the Cyber Security Cooperative Research Centre (CSCRC), published the Cyber Security Governance Principles (the Principles). The development of the Principles reflected demand from AICD members for practical guidance for directors on how to govern cyber security, engage with management and build their own expertise. Until the

publication of the Principles, there was a clear gap in guidance for Australian directors, with existing materials focused largely at a management and operational level.

The Principles are a practical framework for effective board oversight of cyber security across five key areas, including building a cyber-resilient culture, and preparing and responding to a significant cyber incident. The Principles can be applied by organisations of all sizes and sectors, and are brought to life by five case studies from senior Australian directors. For example, Telstra Chair John Mullen (former Toll Group Chair) provides a sobering reflection of his time leading Toll Group through crippling cyber attacks in early 2020, and how Toll's solvency was threatened.

Accompanying the Principles is a one-page checklist for NFP and SME directors, which provides a simple set of low-cost steps that a board can take to enhance cyber resilience, and, separately, a snapshot that includes 10 questions for directors to ask themselves and their management teams. The Principles is a living document, and the AICD and CSCRC are committed to updating it as the cyber security environment and regulatory landscape evolves.

In a welcome sign of endorsement from government, the Principles were launched at a round table with Minister for Home Affairs and Minister for Cyber Security Clare O'Neil MP, experienced practising directors, representatives of government agencies, and cyber industry experts in Melbourne on 20 October 2022. The Principles also include a foreword by the Minister.

The demand for the Principles, and the accompanying SME and NFP checklist,

has been unprecedented, with more than 15,000 downloads in total by February 2023. Separately, we have received feedback from directors utilising the Principles in board meetings to engage with management in testing cyber resilience and to identify areas requiring enhancement. The real-world impact of the Principles is a clear demonstration of how directors are not only motivated to grapple with cyber security risk, but also to take steps to build cyber resilience.

Directors seeking greater support from government

The data breaches at Optus and Medibank in late 2022 generated significant public concern, and have provided momentum for the government to enact policy reform focused on data management and protection at Australian organisations. While the AICD recognises that a measured strengthening of privacy obligations, including the penalty regime, is appropriate, we are concerned that there is too great a focus on the punitive or 'stick' elements of cyber security and data reforms.

Directors report that the existing complex and fragmented cyber and data regulatory landscape is often a barrier to an organisation effectively responding to significant cyber incidents, and ensuring appropriate communication channels exist with government. We have consistently heard from members that boards are seeking partnership and support from government and key regulators on cyber security and data governance, and have strong concerns about the government's focus on layering further prescriptive cyber-related obligations onto businesses of all sizes, adding to the current patchwork of legal and regulatory requirements.

Key areas in which directors have been calling for government support include:

- greater government coordination across future cyber security and privacy reforms
- clarity on regulator responsibilities when undertaking investigations and enforcement activity on cyber security and data breaches
- consideration of how existing reporting and notification obligations can be harmonised or streamlined with the goal that, in the event of a material cyber security or data management event, a business only needs to report or notify the government once
- targeted support for SMEs and NFPs to build cyber security resilience and improve data management practices, including education and assistance in the event of experiencing a cyber security incident
- addressing urgent skills shortages in technology and cyber security specialties
- proactive threat and intelligence sharing by key government agencies with industry.

The AICD genuinely believes that a 'team Australia' approach to building cyber security resilience is possible, with directors demonstrating a commitment to enhancing how the private sector tackles cyber security risk. A focus by the government on support for organisations of all sizes, combined with measured legislative reforms, has the greatest potential to produce results that are of benefit of the Australian community. •

The AICD-CSCRC Cyber Governance Principles can be downloaded here: aicd.com.au/risk-management/framework/cyber-security/cyber-security-governance-principles.html

Australian boards and CISOs lack alignment on cyber

BY YVETTE LEJINS, RESIDENT CISO – ASIA PACIFIC AND JAPAN, PROOFPOINT

With the rising dependency on digital resources, cyber attacks are increasing in both frequency and impact. There are many external challenges facing Australian organisations as they address cyber risk, but a significant one is also internal – the lack of alignment between boards and CISOs.


Yvette Lejins

Cybersecurity: The 2022 Board Perspective, a recent report by Proofpoint and Cybersecurity at MIT Sloan (CAMS), found that only 58 per cent of Australian businesses view cyber security as a top priority, and only 54 per cent of Australian board members believe that they have a clear understanding of the current threats they face.

This indicates that Australian organisations are extremely vulnerable to cyber attacks, and that the issue must become a boardroom priority for more companies. The recent high-profile data breaches dominating the headlines in Australia have highlighted the risks facing Australian companies, and are taking the issue of cyber risk to the board level.

Greater cyber awareness needs to be developed across Australian organisations – the required behavioural changes cannot come quickly enough. The most effective cyber security awareness programs are built from the top down; but when it comes to the modern threat landscape, CISOs and their boardroom colleagues do not always see eye to eye. In Australia, 63 per cent of board members report seeing eye to eye with their CISOs, but just 58 per cent of CISOs feel the same.

Boards underestimate risk

When evaluating the risk posed by today's sophisticated cybercriminals, 52 per cent of Australian board members believe that their organisation is at risk of material cyber attack in the next 12 months, compared with 68 per cent of CISOs. This indicates that too many Australian board members are underestimating the risk of cyber attack. Board members in Australia ranked email fraud/business email compromise (BEC) as their top concern (44 per cent), followed by supply chain attacks (32 per cent), and cloud account compromise (28 per cent). Australian CISOs ranked insider threat, email fraud/BEC, and supply chain attacks as their top concerns.

A lack of harmony at this level can significantly impact an organisation's security posture. Buy-in and investment for new strategies can suffer when CISOs and other board members are not on the same page. Without a clear and agreed upon strategy, attempts to build a security-aware culture at all levels are destined to fail.

While it is ultimately up to the board to take steps to keep cyber security high on the agenda, the CISO has a responsibility to bridge this gap, too. CISOs must deliver concerns, strategies and recommendations in a business-first manner, avoiding jargon and overly technical language. It is a business problem first and foremost, and the language to the board must resonate and provide insight into the real risk profile.

Understandably, board members are less interested in threat detection metrics than in how security awareness can protect revenues. So, by speaking the same language, CISOs can help board members better understand the reasoning behind their suggestions – and better protect the organisation as a result.

Boards lack an understanding of systemic risk

Not only does awareness not always equate to understanding, but it often fails to translate to preparedness, as well.

While over half of Australian board members feel their board understands their organisation's systemic risk, 72 per cent think they have invested adequately in cyber security, and 56 per cent discuss cyber security at least monthly, cyber defences remain insufficient. This lack of cohesion extends beyond the boardroom, as high levels of awareness do not appear to protect against human error, either.

Sixty-two per cent of survey respondents believe that their employees understand their role in protecting the organisation against threats; however, around the same number of Australian board members still believe that human error is their biggest cyber vulnerability. This suggests that while most users are aware of common threats like phishing and malware, they are ill-equipped to deter them in the real world.

Instilling a more granular level of threat awareness throughout an organisation is only possible through long-term, targeted security awareness programs. Education must go beyond standardised tests and tick-box exercises. Every user must fully understand how they are likely to encounter threats in the real world and what is expected of them when they do. No

user is equal, and programs to drive the desired positive behaviour changes need to recognise this.

If businesses are to successfully nurture this kind of security culture, the disconnect between CISOs and other board members must be addressed.

A strong relationship between cyber security and other business functions at the top level will soon be reflected throughout the workforce. The clearer the communication in the boardroom, the greater the understanding of cyber security across the company, and the safer the organisation. Australian organisations need to bridge this gap, as the cyber battle is best fought when boards and CISOs are in harmony, and their strategies are aligned. •

Proofpoint commissioned a survey of 600 board members at organisations with 5000 or more employees across 12 countries: the United Kingdom, the United States, Canada, France, Germany, Italy, Spain, Australia, Singapore, Japan, Brazil and Mexico. Working with researchers at MIT Sloan's research consortium, Cybersecurity at MIT Sloan (CAMS), Proofpoint analysed responses and summarised the insights. It also compared some of the results to corresponding findings from the recent Voice of the CISO Report.

To download Cybersecurity: The 2022 Board Perspective report, please visit www.proofpoint.com/au/resources/white-papers/board-perspective-report

Assess your **Essential Eight**

Empower your organisation to stay ahead of cyber threats by adhering to the **Essential Eight**. Choose a product that provides in depth analysis of your implementation of the Essential Eight strategies and enables you to identify and fix configuration issues.

How do you check "Your Eight"?

The threat of cyber-attack is a persistent and growing concern for organisations of all sizes and industries. The Australian Cyber Security Centre (ACSC) has developed a set of strategies, known as the "Essential Eight", to help organisations protect themselves. These strategies include:

1. Application Control
2. Patch Applications
3. Configure Microsoft Office macro settings
4. User Application Hardening
5. Restrict Administrative Privileges
6. Patch Operating Systems
7. Multi-factor Authentication
8. Regular Backups

These strategies are designed to counteract the most common and severe cyber threats, and they have been shown to be effective in reducing the likelihood of a successful attack.

Are your controls working?

If you have implemented the Essential Eight mitigation strategies... how do you know they are working effectively?

Manual audits often use contractors who are unfamiliar with your environment, or tie up your IT staff, most probably draw conclusions from a subset of your computers, and present you with varying degrees of success and certainty.

...or you could use automated audits

Using automated audits to check the compliance of your controls means that:

- All your computers and servers are audited and not merely a sub-set
- Your computers can be checked on a regular schedule, without consuming resources
- The most recent, updated standards from ACSC can be tested for compliance
- The results are independent of local opinion, with no opportunity for bias or interpretation
- Results across multiple divisions or locations have the same standards and rigour applied
- It is significantly more cost effective than employing consultants

Automated audits provide you with a summary of results on a regular basis, allowing you to focus your organisation's resources on remediation of controls not properly implemented.

Remediation is easy, right?

ACSC's Essential Eight Maturity Model is well defined and provides good guidance on the controls to implement at a high level to reach your desired level of cyber maturity.

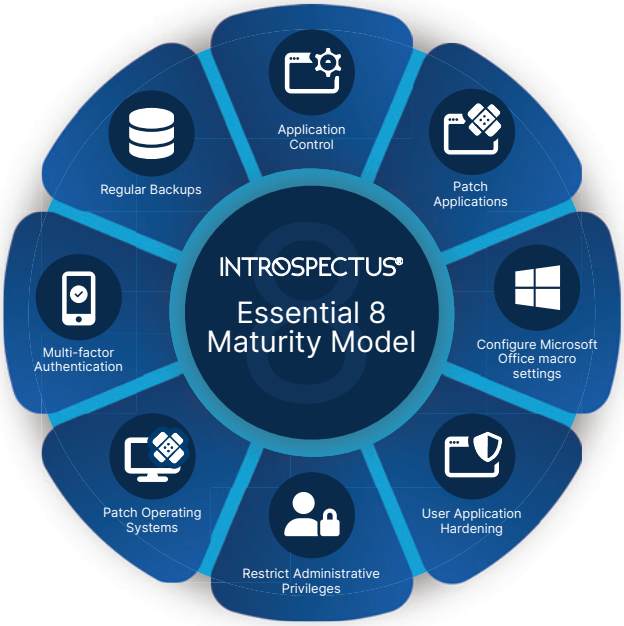
But not all environments are the same!

How do you ensure that the controls are set correctly and rolled out to all end-points in your network?

Automation should provide useful, meaningful and actionable advice for any end-point that is not meeting the Essential Eight requirements.

Look out for tools that provide an easy to use interface with:

- high-level maturity compliance reporting (management or board reporting), and
- the ability to drill down to the individual end-point, with enough detail to understand exactly where the error is and, ultimately, where you need to go and what you need to fix it.



In conclusion

ACSC's Essential Eight controls help organisations to protect themselves against cyber-attacks.

While manual audits may give you some insight into your organisation's cyber maturity, only an automated audit will provide you with ongoing, real-time assurance that your Essential Eight security controls are in place and actually working.

Remember, it only takes one non-compliant computer to bring chaos to your whole organisation

For more information or to organise a demonstration, visit...

introspectus.com.au/assessor

INTROSPECTUS®

Continuous. Unobtrusive. Real-time.

The rise of spear phishing attacks

The secondary impact of recent data breaches is likely to be more highly personalised spear phishing attacks. It's what happens once phishes are received that matters, writes BeyondTrust's Director, Solutions Engineering Asia Pacific, ***Scott Hesford****.*

Concerns about spear phishing have been heightened by recent high-profile data breaches in Australia and regionally, which resulted in the loss of personally identifiable information (PII).

With the information that attackers can readily access on people, increased vigilance is required. Whether public or leaked, data is used by criminals in highly targeted campaigns against specific individuals. This is known as spear phishing.

Spear phishing is one of the top 10 most common social engineering attacks. Attackers research their target and highly personalise the outreach to make it more convincing. The attacker uses information only the target would potentially know or recognise as legitimate to create a perception of trust.

Leaked data, on top of publicly accessible sources – such as business social media profiles – can help attackers craft convincing campaigns against business leaders, their direct reports, or partners.

Blurred lines

A renewed area of concern is the extent to which PII stolen in consumer-oriented breaches can be used as part of an attack against business interests.

As the Australian Cyber Security Centre (ACSC) notes in its most recent threat report, 'The blurring of work and home lives has made the information held by individuals more valuable to malicious actors. Email accounts listed in PII holdings will almost certainly be under increased threat of spear phishing activity.'

The normalisation of the work-from-anywhere environment has increased the number of employees who are remotely accessing network resources, the number of unsecured remote locations from which they may be accessing those network resources, and the number of systems and sets of login credentials that a single user needs in order to work effectively.

Laptops offer a broad attack surface with many potential opportunities for exploitation. Businesses find these devices hard to secure: 89 per cent of respondents to a survey we ran at last year's AusCERT conference said that securing remote workforces remains a challenge.

Attackers are making the most of the opportunity: 59 per cent of identity-related breaches in the past year were caused by phishing (encompassing both broad-based campaigns and spear phishing). This is the single largest category of identity-related breach, and is over 20 per cent higher than for any other potential vector.

Fake invoices

A common example of a well-crafted spear phishing campaign is false billing or fake invoice scams.

They're the second most reported type of scam in Australia, and are ranked fourth highest by loss amount – in the order of

Scott Hesford

$20 million in 2022 alone. As potential losses can run into tens of thousands of dollars or more per target, it is likely that these numbers are fairly conservative; they show only the attacks that are reported to authorities. Some go unreported, and the losses are simply absorbed to avoid the possibility of public embarrassment.

Clearly, some of these phishes are tailored to be very convincing.

A steady stream of PII stolen and leaked via data breaches is ensuring that attackers can continuously hone their targeting. The more targeted and personalised they get, the higher the chance that a person slips up and is convinced to engage with a spear phishing attack.

Not training alone

Detection and mitigation of these threats can't all be left to individuals alone. While many organisations put staff through cyber security awareness training and simulated tests so they can better recognise potential phishing attacks, it is hard to move the needle. The failure rate of simulated tests is fairly consistent year on year.

People have lapses and make errors. A tired, busy or otherwise distracted user may not apply the same rigour to a suspicious email that they ordinarily would. It takes only one such mistake to give a cyber intruder a foothold in their computer, and a place from which they can move laterally to inflict greater pain on the employee's organisation.

Rather than rely solely on people, technology is an important additional layer of defence and mitigation against the rise of spear phishing, and phishing attacks in general.

Three technology-based defensive layers are recommended to address or mitigate the threat posed by spear phishing attacks:

1. Remove local administrators

It's all too common that users have administrator rights on local assets, which puts the entire enterprise at risk. According to the BeyondTrust Microsoft Vulnerabilities Report, 2015–2020 findings indicated that as many as 75 per cent of critical vulnerabilities could have been mitigated by removing admin rights. As such, removing local administrators and instead performing just-in-time privilege elevation alongside application control should be used as a quick time-to-value solution for increasing productivity and security at the same time.

2. Multi-factor authentication

Multi-factor authentication (MFA) requires users to identify themselves with two or more unique factors – something they know (such as a password or PIN) and something they have (such as a hardware or software token) – before they are granted access to sensitive systems. Enforcing MFA within an environment – whether it be on a login before the use of a privileged account, third-party access or even running a specific application or task – will help mitigate the threat of stolen credentials.

3. Application control

According to the BeyondTrust Malware Threat Report 2021, over 90 per cent of malware enters organisations via Microsoft Office documents and workbooks. Blocking untrusted scripts or macros from being executed by Excel or Word also helps to reduce the threat of malware entering an organisation following an initial attack. This is supported by current ACSC guidance for mitigating the risks of phishing and spear phishing attacks. •

E-safety: Is your household standing on a wobbly stool?

BY NICOLE STEPHENSEN, PARTNER, IIS PARTNERS

The three-legged stool is a helpful analogy when explaining the concept of safety in online environments (e-safety) to families. It would be risky to stand on the stool if any of the legs – safety, privacy and cyber security – were to be wobbly or missing!

Safety is when a person is protected from danger, risk or injury. To increase safety in online spaces, the other two legs are vital.

Privacy is concerned with personal information; that is, information about a person that identifies them, could lead to them being identified, or could allow them to be tracked, traced or targeted.

Parents, do your kids know what their personal information is and how much of it they are sharing online? It includes their name, how to contact them (address, phone number, email address, their coordinates on the socials), where they go to school, who their friends are, whether they are sick or well, their age, their ethnicity, and their religious beliefs. Then there's the digital stuff, like usernames and passwords, location data (that's where they are on the map when using their phones and certain apps), web-browsing patterns, purchase history and preferences.

It also includes their image. Faces are uniquely identifying, and yet people of all ages are allowing apps – many of shifty origins – to access, use and store their faceprint to create cute gaming and social media avatars, and sexy artificial intelligence artwork. Imagine for a moment millions of faces, mapped back to other identifying details, stored in databases accessible to (and maybe even built for) foreign governments in the guise of 'online amusement'.

Cyber security is another facet of safety online. Many people use services to protect the device they use, or their online accounts, from hacking and other forms of deliberate cyber attack. That's important, but hacking is not the thing I worry about most when it comes to young people. For them, hacking

Nicole Stephensen

happens in the movies and involves hipsters in hoodies.

Keeping security closer to home as a preventive activity is helpful for reinforcing behaviours such as not sharing username and password details with people they don't know over the phone, via email, or in online chats; limiting who can view their posts on social media to 'friends' only; covering their phone camera or webcam with a sticker when they are not using it; and not sharing their personal information in games, chats, online surveys, pictures, and videos.

For parents, this includes moving away from 'sharenting'; peppering the socials with pictures of your naked baby in a basket and child's first day of school, book week, eisteddfod and goofy video outtakes only increases their digital footprint, and limits your control over what happens to those images once they are out there.

What is shared in online spaces can impact safety in offline spaces. Kids sharing details of your next family camping trip before you go reveals that no-one will be home for a few days. You may all return to find that your house has been burgled! Videos, shorts and picture posts to the socials can reveal where you live, where your children attend school and who their friends are. Sharing personal information with strangers in game chats could place kids in the sights of sexual predators, who are skilled at extracting mobile numbers, email addresses, locations and images from their targets.

Checking the legs of your stool

Whenever we have time on our hands, it's a chance to catch up on that to-do list around home and finally take care of the things we've been putting off – like completing those helpful checks around safety, efficiency and environmental sustainability. An energy usage check, for example, can be a real eye-opener about electricity use at home, and can identify smarter choices such as switching the type of light globes you use, moving away from energy-sucking appliances and using your daytime solar feed a little more wisely.

On the face of it, you may consider an online safety check to be lower on the totem pole than other safety-related checks like bushfire or flood preparedness, storm readiness, vehicle roadworthiness or coping during a power outage. But when you think about the three-legged stool your family is standing on – and the the very real issues of identity theft, online abuse and bullying, unwanted marketing, unwanted tracking through apps and technology-facilitated exploitation of children – you might prioritise this check after all.

To check the legs of your stool:

- Do an inventory of all the tech you use in your household. This includes all your devices (e.g., laptops, tablets, phones),

gaming devices (e.g., PS4, virtual reality), smart TVs, home assistants ('Hey Google!'), smart toys and surveillance devices (e.g., doorbell, baby monitor), and connected home appliances and wearable gadgets (e.g., smart fridge, robot vacuum, watches).

- Write down what the tech does for you, how it helps you or the purpose it serves. For example, does it recognise your voice and communicate with you? Take pictures of you or the space you are in? Record what you are doing? Place orders or spend money on your behalf? Know your likes, dislikes, tastes or preferences?
- Think about the ways you actually use the tech. Have you enabled family-sharing across a number of devices? Do you access services like YouTube, Netflix or internet browsing from your smart TV? Are you using the tech for gaming when you initially bought it for homeschooling?

- Identify your potential pain points. These are things that raise red flags for you. For example, do your kids purchase content via the iTunes account linked to your credit card? Is your laptop used for personal and work purposes? Are your kids unsupervised while gaming? Are devices allowed in bedrooms?

Once you've completed your check, it's time to tighten the legs of your stool by setting rules around how you and your family use technology, and address things that concern you.

Standing on the stool safely

The 'red flags' part of your online safety check is a vital reference point; however, many households don't immediately spot them. A few worth noting include:

- stored credit card details in iTunes, Amazon and similar accounts without two-factor authentication enabled for any purchases
- young people using phones, tablets or laptops in their bedrooms – some text, email, chat and video activity is too risky to be unsupervised
- a long time between updates (which often address security bugs) on the software and apps you regularly use
- kids having gaming, music, email and other accounts when they are under the minimum age set in the provider's terms and conditions

- anxiety about needing virtual currency (gaming money) or online status items (like 'skins' for a character) in order to avoid bullying in the real world
- technology neediness generally in the household – that is, being unable to feel happy or relaxed without being 'connected'.

Try taking this simple three step approach:

1. Reflecting on your tech inventory, decide what technologies you need (or want to continue using) in your household. Most folks would rather not part with the tech once they have it, but this is still an important step. It helps you focus on just how many devices, gadgets, accounts, socials and apps are in your life (and just how much personal information is involved when you use them).
2. Set some safe-for-use rules in relation to the technologies, keeping those red flags you've identified in mind. This involves having age-appropriate conversations about online safety, which can sometimes be challenging or awkward. Tapping into the resources offered by the eSafety Commissioner can really help with this. Rule-setting in households with children is not always going to be democratic, but young people are wonderful at determining (and self-monitoring) rules that support their own safety... so involve them! There is no one-size-fits-all approach to this step; however, an effective starting point could include deleting unused apps after 60 days; that only the adults in the household can press 'buy now'; that kids nominate a trusted adult to tell any online worries to; and that everyone will follow the 'stop, block and tell' rule if they experience online bullying or abuse.
   This step also involves essential housekeeping, like ensuring your family-share permissions for devices and accounts are still appropriate; installing device security updates when prompted; subscribing to security alerts issued by the Australian Cyber Security Centre; and checking for your email addresses and credentials that might have been compromised at www.haveibeenpwned.com.
3. Stick to your rules... and don't be afraid to revise or refine them as your household ages and technology changes. •

Get future ready

BY JINAN BUDGE, VP AND PRINCIPAL ANALYST, FORRESTER

From security awareness and training, to adaptive human protection (via human risk management).

Jinan Budge

The security awareness and training (SA&T) market has been stagnant for so long, with the last major disruption (as far as I can tell) being the introduction of phishing simulations about a decade ago. Since then, the industry seems to have seen a slow and steady evolution – from ticking boxes to meet a web of uninspiring security training requirements imposed by security frameworks and regulations, to 'better' content and ways to assess users via games, simulations, quizzes, and other 'better' training techniques.

After four years of research into this market – receiving hundreds of vendor briefings; running dozens of strategy days and hundreds of discussions with CISOs and security leaders via inquiries, round tables, or speaking engagements; and sifting through thousands of lines of vendor responses to my questions in our two Forrester Wave™ evaluations of SA&T[1] – I finally see a well-needed disruption, and I love disruption!

In September 2022, Forrester's guide to global SA&T regulations and standards[2] revealed an impetus for a better future. In November 2022, we unveiled new research in The Future Of Security Awareness And Training report[3], which examined the major expected changes in security awareness and training in the short, medium and long term.

In the long term, adaptive human protection will create freedom for employees

A widely accepted cyber security mantra is that 'security is everyone's responsibility' – but the goal of adaptive human protection is to move past that. This starts by instilling a security culture, eliminating needless compliance activity and adding capabilities so that humans will be hard-pressed to make wrong decisions. This allows you to imagine a future in which you can safely jettison practices that were once required but are now superfluous. Once cyber security is no longer everyone's responsibility, employees can get on with their daily activities and meet their digital aspirations while remaining protected from cyberthreats – even if they make a mistake.

The thing is, this future is realistically 6–10 years away for most. In the meantime, cue human risk management.

The medium-term focus on human risk management will overcome SA&T's shortcomings

Make it the goal of the SA&T program to positively influence employee security behaviour, instil a security culture, and manage human risk by taking six crucial steps:

1. Expand your behavioural baseline beyond phishing and incidents.
2. Measure effectiveness, not completion.
3. Quantify the human risk based on behaviour (not scores).
4. Initiate real-time, risk-based interventions.
5. If you must use content, be intentional and transformative.
6. Codify security culture.

The immediate term has us focusing on the methods by which we train people, rather than the outcomes

The regulations and standards that have, to date, driven SA&T programs are often outdated and confusing, and have compelled companies toward compliance as a strategy. Today, most organisations measure their success in SA&T by measuring completion or phishing click rates, instead of actual behaviour or culture change, while providing perfunctory content-driven awareness programs. This leads to a learn-and-dump approach to security, does not address underlying security process and technology issues, wastes everyone's resources (including and especially your employees'), and perversely increases risk (due to being hated by everyone).

Disruption is well needed. We don't have the luxury of ignoring the human element in security – every security control has a human element. And we certainly can't continue to address it in the way we have done so in the past – by training all the people on all the things all of the time. We all have limited resources in this life, at work and beyond, and we need to be smart, creative and adaptive about it. •

References

1 https://www.forrester.com/blogs/you-say-you-want-a-revolution-announcing-our-latest-security-awareness-training-wave/

2 https://www.forrester.com/report/forresters-guide-to-security-awareness-and-training-regulations-and-standards/RES177897?ref_search=0_1676433408219

3 https://www.forrester.com/report/the-future-of-security-awareness-and-training/RES178339

Australian boards must address the material risk of cyberthreats

BY JO STEWART-RATTRAY, INFORMATION SECURITY ADVISORY GROUP, ISACA

Following the high-profile data breaches at Optus and Medibank Private in October, it is clear that for board members and directors to meet their obligations to customers and shareholders, they need to better understand and address the material risks arising from cyber security failures.

The recent data breaches impacting millions of Australians have shaken consumer confidence and motivated government to act decisively. As a result, boards and directors can expect greater scrutiny and penalties.

Whether a breach is the result of poor business practices or criminal activity, the responsibility to protect sensitive and private data is no longer the sole purview of the CISO. Boards, directors and security experts will all be judged on their understanding of,

and response to, material risks arising from unintended data breaches and more frequent, malicious cyberthreats.

Material risk, including financial impact and reputational damage, is growing.

Financial risk

Where customer data was previously considered an asset, boards should view unprotected data as a potential liability. Beyond the financial risk in terms of lost revenue, which can be significant, boards must also consider the high costs of remediation, compensation and possible legal action. Privacy breaches may require consumer compensation, for example, to cover the costs of new identification documents. It is possible that more serious customer losses due to fraud could result in costly legal action.

Organisations should also prepare for greater financial penalties if they fail to protect customer privacy. Strengthening the powers of the Australian Information Commissioner and the Notifiable Data Breach Scheme, the government intends to introduce legislation to increase penalties for repeated or serious privacy breaches. The penalty introduced for parliamentary consideration increases from $2.2 million to $50 million, or three times the value of any benefit obtained through misuse of information, or 30 per cent of a company's adjusted turnover in the relevant period – whichever was greater.

The Office of the Australian Information Commissioner's report on notifiable data breaches from January–June 2022 indicated that malicious and criminal attacks were the largest source of data breaches at 63 per cent. Ransomware accounted for the highest number of cyber security incidents at 31 per cent. There is no doubt that ransomware payments and cyber insurance will be hotly debated in government and boardrooms across Australia.

Reputational risk

The experiences and perceptions of consumers in relation to cyberthreats and the organisations they engage with correlates directly to material risk for an organisation's reputation, financials, competitiveness and potential for growth.

With a growing sense of desperation among consumers who think nothing can be done to protect them from cybercrime – as highlighted in ISACA's Consumer Cybersecurity 2022 survey – boards and security professionals need to act.

What should be of most concern to boards is that once trust is lost, consumers may sever ties with the business, resulting in lost revenue and reputational damage. The ISACA study indicates that Australian companies with compromised cyber security are at risk of losing one in four customers. When consumer trust falters, the business falters.

With threats increasing in both frequency and sophistication, it is imperative for board members and directors to broaden their knowledge of cyber security, and better understand the material risks to their organisation.

While 82 per cent[1] of security professionals are confident in the ability of their cyber security team to detect and respond to cyberthreats, 23 per cent of consumers are not confident that a business can secure their personal identifiable information. Although not a direct comparison, it highlights the importance of board members understanding an organisation's cyber strategy and capabilities.

Boards must engage more closely with the security professionals who play a critical role in bridging the gap between the consumer experience and perception of cyberthreats, and the organisation's ability to protect them from, and respond to, cyber attacks. It's time for the CISO to have a seat at the table. •

About the author

***Jo Stewart-Rattray**, CISA, CRISC, CISM, CGEIT, is a member of the Information Security Advisory Group (ISACA); Vice President – Community Boards, Australian Computer Society; and Director, National Rural Women's Coalition. She has more than 25 years of experience in the security industry, and consults on risk and technology issues, with a particular emphasis on governance and IT security in businesses as the Director of Technology and Security Assurance with BRM Advisory. Stewart-Rattray regularly provides strategic advice and consulting to the banking and finance, utilities, healthcare, manufacturing, tertiary education, retail, and government sectors.*

1 State of Cybersecurity 2022, Figure 32

Resist the currency of fear

BY JOYCE HARKNESS, DIRECTOR, CYBERSECURITY FOR ANZ AND ASIA, ISG

How to make sound cyber security investment decisions using risk quantification.

Joyce Harkness

After widely publicised cyber security incidents in Australia – such as the data breaches at Optus and Medibank, not to mention global incidents like the SolarWinds breach – there is often a spike in attention on the organisation's vulnerability to similar attacks, and whether the right investments have been, and are being, made. Sometimes, you hear commentary that it's time to take advantage of the new heightened interest and ask for more funding for cyber security.

But as time has shown, the currency of fear is not a lasting influencer of cyber security investment decisions. Over time, the memory of the incident and the urgency recedes. How many such incidents have we experienced around the world? Remember the 2017 Yahoo breach in which more than three billion user records were breached? Or the 2013 Target breach, in which over 40 million credit card numbers were exposed? Or the 2017 Equifax breach, in which the personal information of 143 million Americans was affected?

And even worse than a fading sense of urgency is when that momentary spike in attention leads to a mash-up of cyber security investments that do not provide enough value in risk reduction, and fall short of enabling businesses to be more agile and grow.

What are we protecting?

In a world with finite resources and a constantly changing business ecosystem, our investment in cyber security must start with one key question: what are we protecting? Only then can we figure out the means and the sequence to implement that protection.

Cyber security is no longer the sole concern of the enterprise. It is now the concern of governments and citizens. We expect that our personal information is at the top of the list of assets to protect, alongside highly sensitive business information.

Reducing viscosity in the flow of delivery of business change: the value of reducing risk

It is difficult to justify a cyber security program based on the traditional ways an investment is made – that is, by the return on investment based on opportunity, revenue and cost drivers. Let's face it, a cyber security program is there to reduce risk and, by doing so, facilitates the speed of business change and growth. This is why differently valued information requires different protective measures. The cost of investment, therefore, should align with the value of reducing the risk to the information.

When budgets are limited, and there are no silver bullets: matching cyber security investment to the value of lower risk

A better way to look at the value of a cyber security investment is by linking the investment to the maturity of the capability and quantifying the risk reduction of doing so. Quantifying the risk in the language of business leaders and boards means going beyond the usual operational metrics, such as number of threats thwarted, and instead measuring the value, in financial

terms, of the business risk being reduced. Consequently, this action enables business growth and agility.

Creating a risk model requires rigour, and deep market data and intelligence to test such models. The model should reflect your specific susceptibility to the risk, and give leaders the ability to 'war game' their investment sequencing and test their capability maturity plan against the enterprise's risk appetite.

A cyber security road map planning session can be powerful when cyber security teams invite interested stakeholders to participate and be part of informed decision-making.

Use this approach whether you are just starting on your cyber security program or are assessing the optimum pathway to reduce business risk where it matters.

Consider reviewing your past investments to get a baseline of the value of the risk reduction so far (and consequently, the value of enabling business growth and agility), then track your cyber security program's impact on risk as you progress.

When things change, as they often do, whether from internal or external forces, you can use this approach to gauge which choice is best for your business going forward.

Quantifying risk: leveraging insurance-type approach to modelling of risk impacts

No-one is impenetrable. It is wise to assume that an organisation or business may experience a breach in the future. It is better to shift the focus from probability to what the level of susceptibility is. Like considerations for taking life insurance, one looks at consequences of an event and what outcome is desired, then calculates the financial value to the items and activities that bring about those outcomes. We can approach the quantification of cyber security impacts in a similar way.

Pull a diverse group together and consider the following when quantifying cyber security risk impacts:

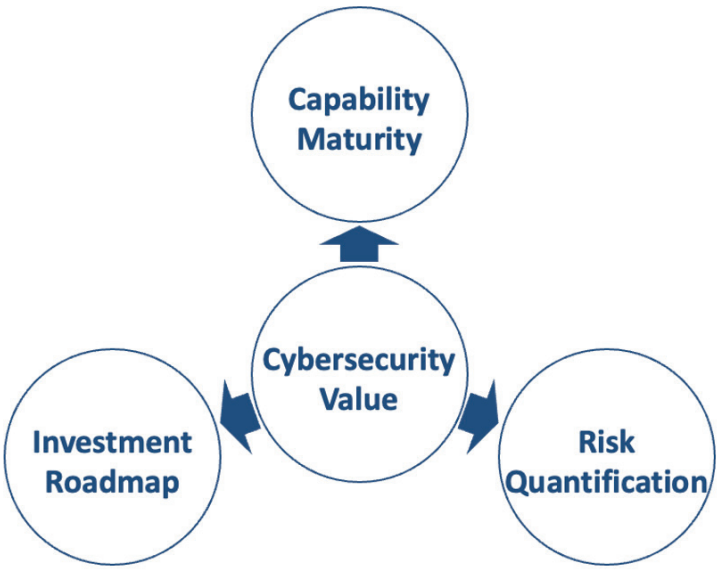
1. *What are the risk scenarios that apply to the organisation?*
   You can find these in risk management reports, crisis management plans, cyber resilience tests, scenarios that other similar companies have experienced, and specific scenarios that impact the unique value and capabilities of the

organisation. Find the who, why and how, and start to describe the scope of the impact on the business, such as what functions and business units will be affected, the proportion of user devices, and the like.

2. *What are the threat objective(s) that apply to each scenario?*
   Common threat objectives include extortion, data destruction, operations disruption, reputation damage and IP theft.
3. *What scenarios would you prioritise to quantify first?*
   Think susceptibility, not probability. Consider multiple impact points and consequences.
4. *For cyber security risks, look at the various impacts – financial, physical and others – within the organisation and with other parties.*
   Examples of financial impacts include ransom payments, forensics costs, and data recovery costs. Examples of physical impacts that need to be translated to financial terms are repairs and replacements, lost income from physical damage to equipment, and the like.

For more comprehensive results, get help from external experts. Look for those who have built these models specific to cyber security, versus other types of business risk.

Figure 1. The Cyber Security Value Model



Ask how mature the algorithms are – that is, the length of time they have been used and tested in the field, and the richness of the datasets captured. Ideally, you would expect the algorithms to have adjusted for modelled impacts against the actual costs if the risks became real and they are known, and the data aggregation to be used in anonymised fashion for you to compare the risk impacts in financial terms against other companies in the dataset.

Beyond capability maturity assessment

The next time you want to assess your cyber security capability or the effectiveness of your cyber security road map and investments, think about how much more powerful that assessment becomes if you link investment planning to maturity growth and risk reduction. This is better than having a proliferation of tools, yet still lacking the maturity to have a significant impact on risk reduction. Imagine how many conversations you will have with highly engaged C-suite leaders when you shift your cyber security investment language to the language of business. Imagine a day when the advocacy for cyber security investments matches the enthusiasm for digital transformation.

How does your organisation approach cyber security investments that require support from many functions and business units?
When a cyber security policy setting is required to meet the risk appetite and regulatory requirements, how are the business and technology changes enabled to adjust to that new setting?

What next for your organisation's cyber security posture?

Well-known management expert Peter Drucker once wrote that 'culture eats strategy for breakfast'. This means you must understand how your organisation thinks, talks and behaves when it comes to risk, including cyber security risk. If you want to know where your culture stands, a risk culture experience assessment is your first step.

You don't have to use the currency of fear to push for additional funding or advocate for support. Simply begin to put cyber security investment decisions in business-relatable terms, so you can articulate value in terms of capability maturity, return on investment, and risk reduction. And, while you're moving to this new cyber security value model, strip away the jargon – the opaque cyber security acronyms and tech speak – and start using generally understood business terms and familiar, accessible language. •

About the author
Joyce Harkness *is Director of the cyber security practice in ANZ & Asia for ISG (Information Services Group). She leverages 30-plus years of leadership experience in whole-of-business transformation, customer operations and information technology to solve complex problems in cyber security. Her overarching vision is that cyber security becomes an enabler of growth, agility, operational excellence and business resilience.*

Overcome the cyber security talent shortage

Now more than ever, cyber security and information security careers are in high demand. The industry is broad and needs a variety of skills, and it is no secret that there is a significant shortage of skilled professionals. Many Australian organisations are recognising the value of developing internal cyber security talent, rather than hiring externally.

In response to the cyber security skills shortage, SANS (the world's largest and most trusted provider of cyber security training and certification) has developed SANS New2Cyber – a curriculum proven to help non-technical individuals who are looking to enter the cyber security field. The curriculum offers a range of courses tailored to building the foundational knowledge and skills needed to pursue entry-level cyber security roles.

The SANS New2Cyber fundamental courses are designed to provide a common set of skills to understand how attackers operate, and how to implement defence in-depth, and respond to incidents to mitigate risks and properly secure systems.

SEC275: Foundations – Computers, Technology and Security
This is the best course to help people with no technical experience to understand the concepts of computers, technology and cyber security. Take a course walk-through and see what this course has to offer.

SEC301: Introduction to Cyber Security
This course offers a balanced mix of technical and managerial issues for students who need to understand the salient facets of basic information security and risk management.

FOR308: Digital Forensics Essentials
The Digital Forensics Essentials course provides the necessary knowledge to understand the digital forensics and incident response disciplines, how to be an effective and efficient digital forensics practitioner or incident responder, and how to effectively use digital evidence.

SEC388: Introduction to Cloud Computing and Security
The purpose of this course is to learn the fundamentals of cloud computing and security. This is done by introducing students to, and eventually immersing them in, both Amazon Web Services and Microsoft Azure. By doing so, SANS exposes students to important concepts, services and the intricacies of each vendor's platform. This course provides students with the knowledge to confidently speak to modern cyber security issues brought on by the cloud, and become well versed with applicable terminology.

SEC401: Security Essentials: Network, Endpoint and Cloud
Learn essential information security skills and techniques to protect and secure critical information and technology assets. This course dives deep into active defence, cryptography, networking, architecture, Linux, security policy, Windows, web security, the cloud, and much more!

SEC402: Cybersecurity Writing: Hack the Reader
Want to write better? Learn to hack the reader! Discover how to find an opening, break down your readers' defences, and capture their attention to deliver your message – even if they are too busy or indifferent to others' writing.

SANS also offers a wide selection of free resources, such as webcasts, YouTube channels, blogs, newsletters and podcasts for anyone interested in getting started in cyber security. ●

Want to know more about developing your team's cyber security skills with the SANS New2Cyber courses? Email ANZ@sans.org or call +61 2 6174 4581 for more information.

SANS | GIAC CERTIFICATIONS

DEVELOP YOUR OWN CYBERSECURITY TALENT WITHIN YOUR TEAM WITH

SANS NEW2CYBER

Cybersecurity and IT Essential Courses

As Australia is experiencing a shortage of cybersecurity professionals, more and more organisations are recognising the value of developing internal cybersecurity talent rather than hiring externally. SANS' mission is to equip your team with the skills they need to succeed.

The SANS NEW2CYBER courses are designed to provide a common set of skills to understand how attackers operate, implement defense in depth, and respond to incidents to mitigate risks and properly secure systems.

SANS New2Cyber courses will focus on:

- Techniques that focus on high-priority security problems within your organisation
- Build a solid foundation of core policies and practices to enable you and your security teams to practice proper incident response
- How to develop effective security metrics that provide a focused playbook that IT can implement, auditors can validate, and executives can understand
- Build an internal security roadmap that can scale today and into the future

SEC275:
Foundations: Computers, Technology, & Security

SEC301:
Introduction to Cyber Security

FOR308:
Digital Forensics Essentials

SEC388:
Introduction to Cloud Computing and Security

SEC401:
Security Essentials - Network, Endpoint, and Cloud

SEC402:
Cybersecurity Writing: Hack the Reader

"This training has given me a great overview of everything security related... showing you such a broad amount of information that you will use to determine security issues you may not have considered before."
—Frank Perrilli, IESO

Want to know more about developing your team's cybersecurity skills?

Contact anz@sans.org for more information | +61 2 6174 4581

New2Cyber Job Roles:

- Security Analyst
- Digital Forensic Analyst
- Security Engineer
- Technical Manager
- Auditor

AUSTRALIAN CYBER CONFERENCE 2023

MELBOURNE | 17 – 19 OCTOBER

Melbourne Convention and Exhibition Centre

DON'T MISS THE **CYBER EVENT OF THE YEAR!**

INTERNATIONAL KEYNOTE SPEAKERS
4,000+ DELEGATES • 400+ SPEAKERS

SUPER SAVER REGISTRATIONS
and Call for Papers
open 22 March 2023

#cybercon2023
cyberconference.com.au

OPPORTUNITIES

AISA